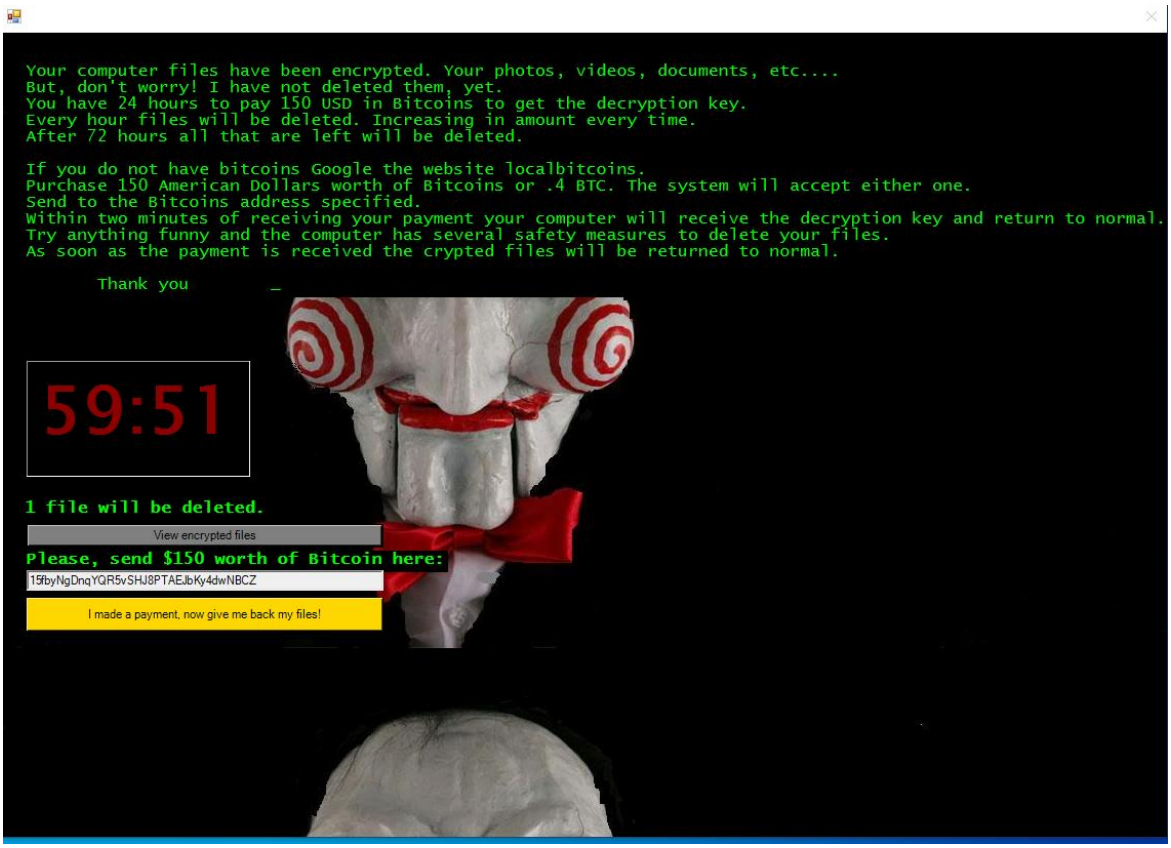
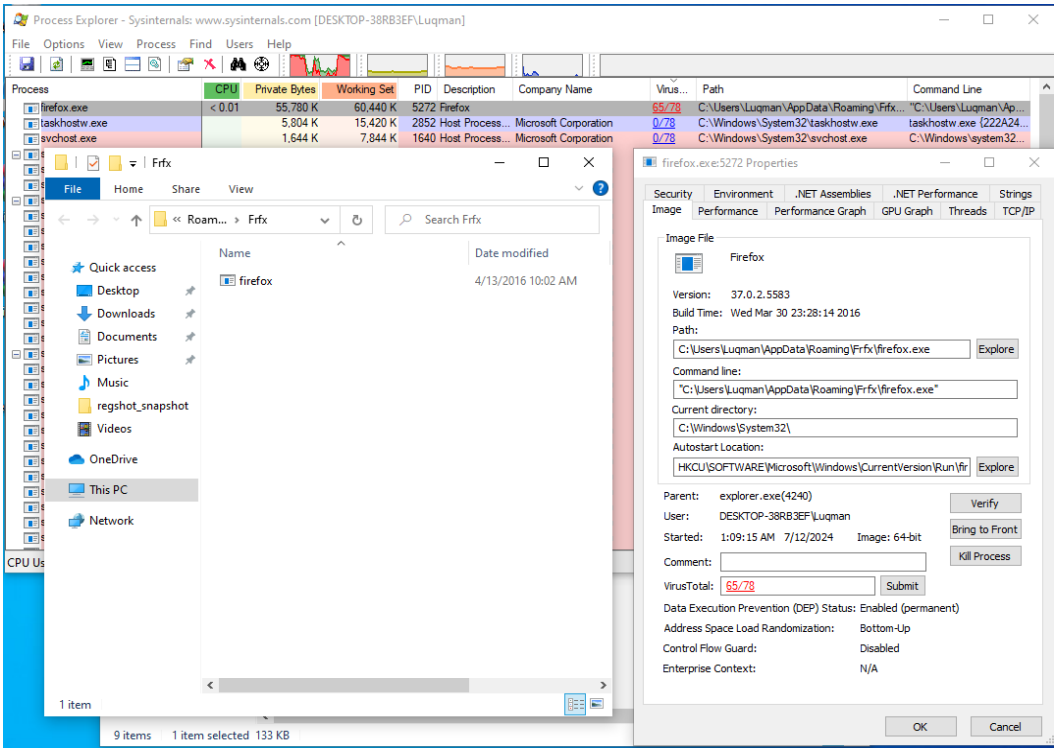
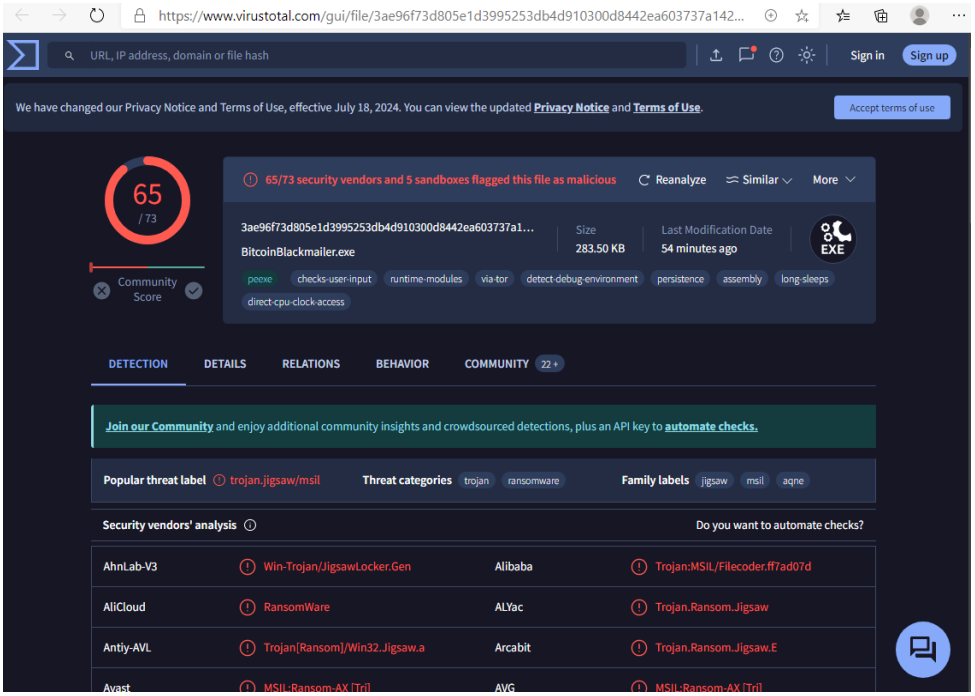
Assessment of Computer for Malware Presence and Threat Evaluation
SIEM & SOC - FINAL PROJECT

Upon starting the computer, the Jigsaw malware launches with a demand for payment, or the encrypted files will be deleted.

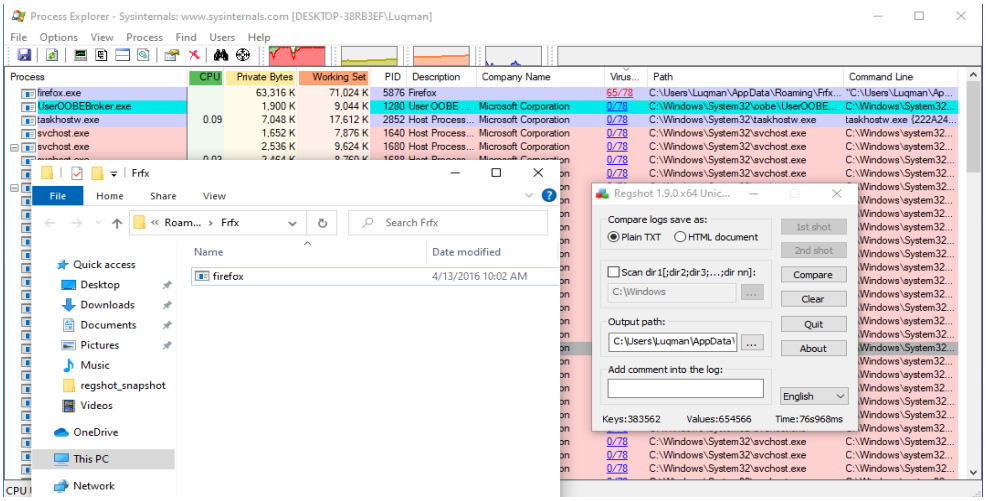


I used File Explorer with an added VirusTotal column, and found the file path. Also checked this file on virus total.

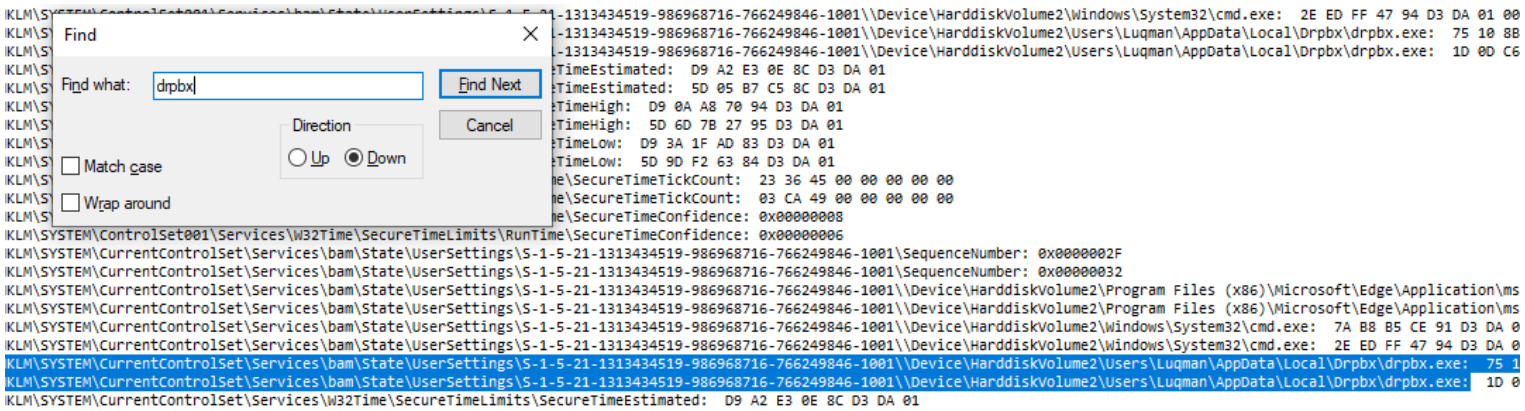


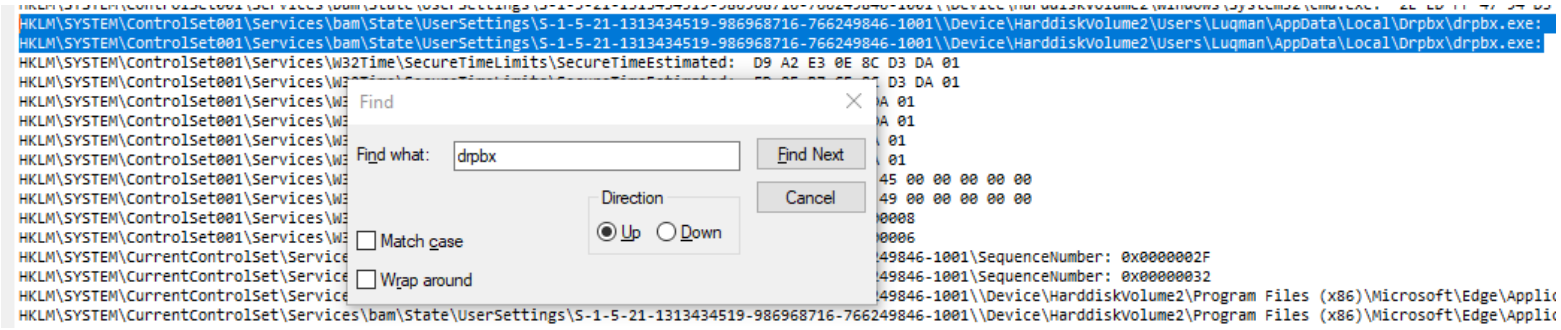


I used a Regshot before and after the Jigsaw malware launched.



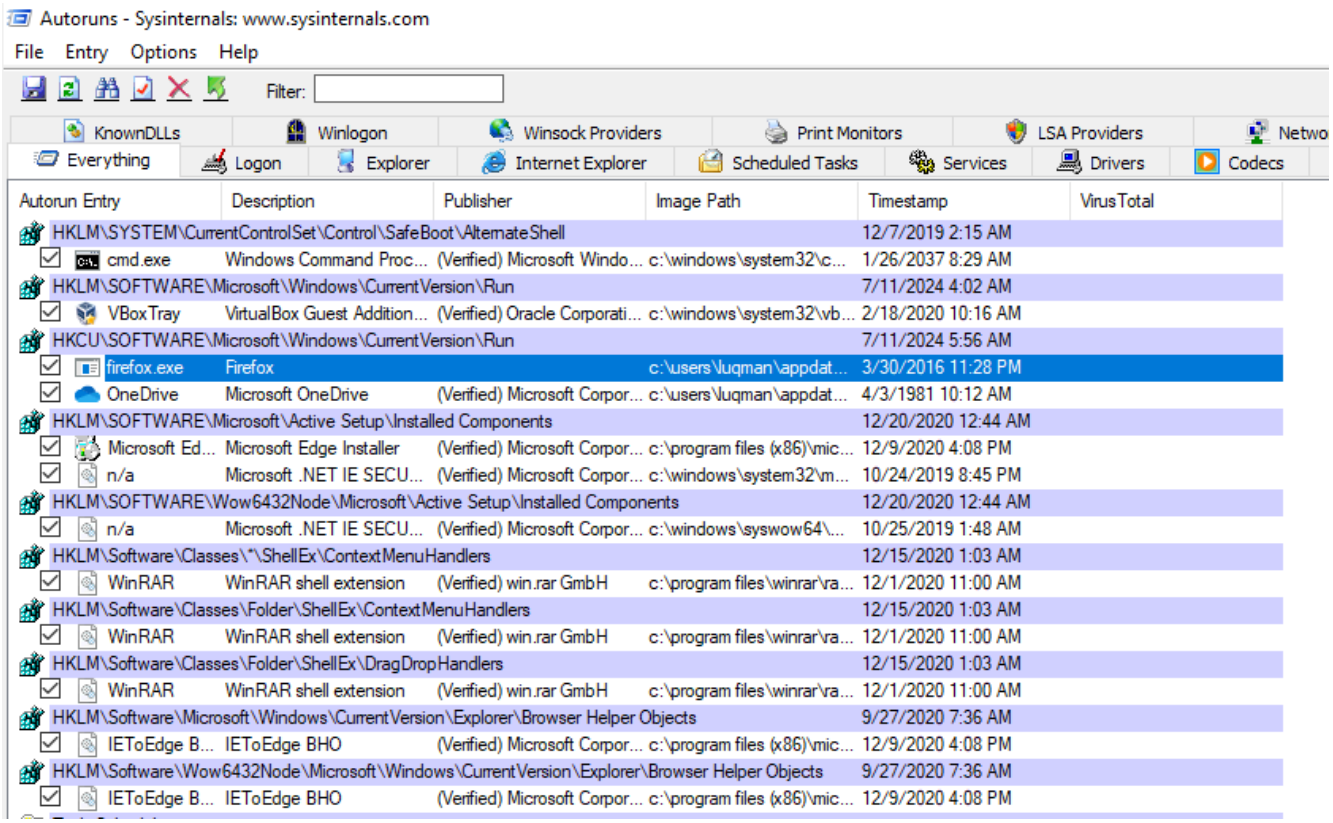
The malware alternately launches the firefox.exe and drpbx.exe processes, both of which perform the same malicious actions.

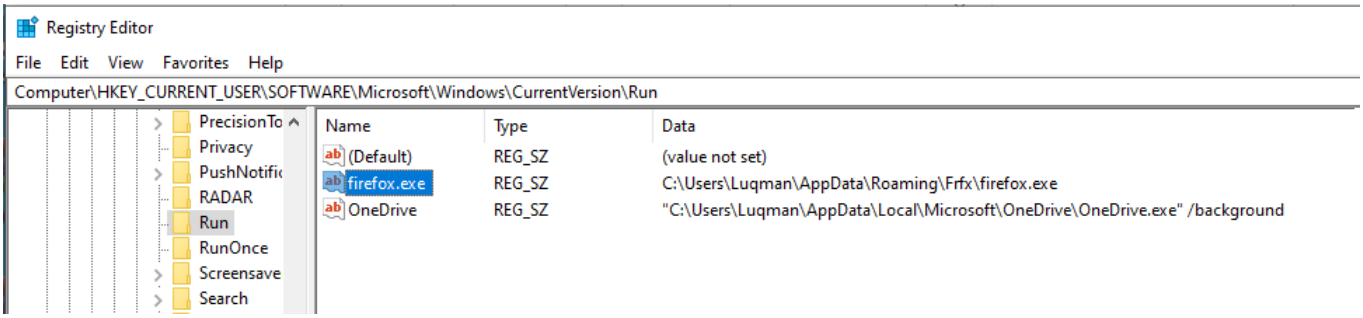




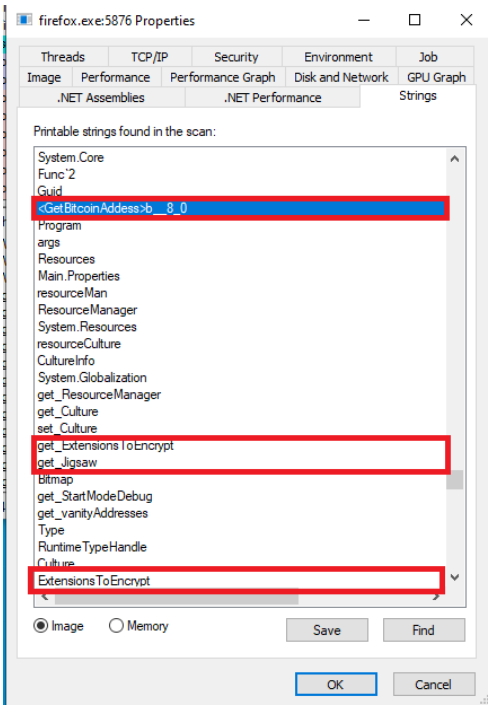
After reviewing the registry files, it was determined that Jigsaw has infiltrated the autorun, causing it to execute upon every Windows reboot.

I used Autoruns from Sysinternals to locate the malicious files.





Next, I examined the strings using File Explorer to prove the malicious nature of the processes.



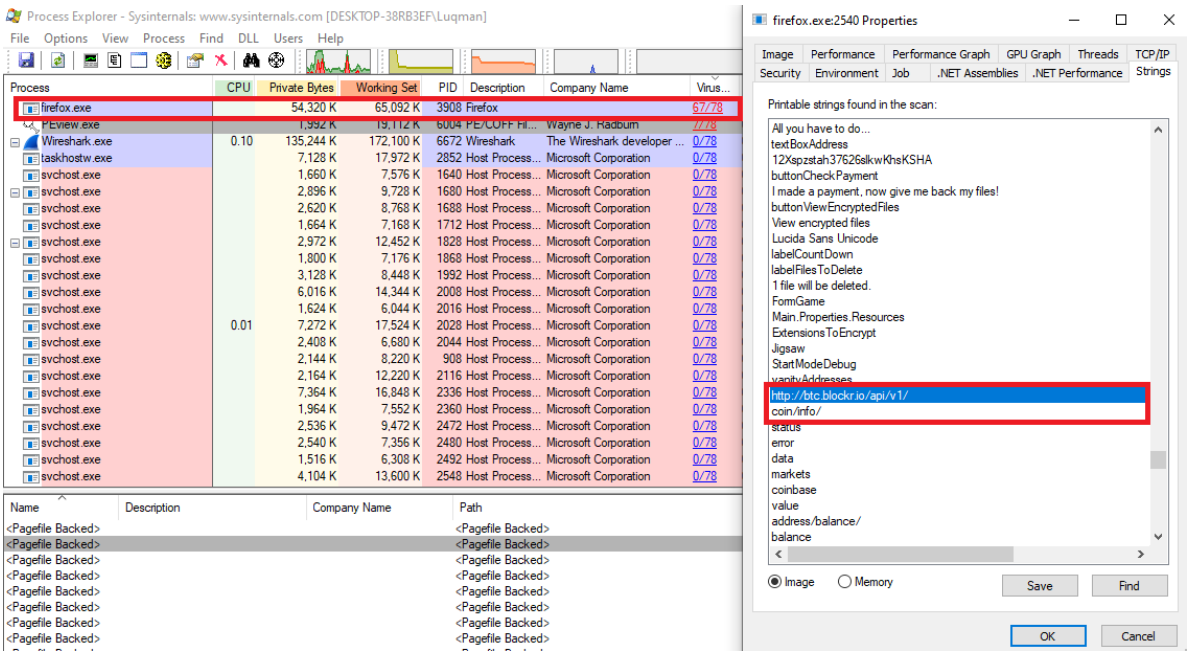
In the meantime, a system error emerged, which could potentially indicate the activity of the Jigsaw malware.

```
See the end of this message for details on invoking
just-in-time (JIT) debugging instead of this dialog box.

************** Exception Text **************
System.IO.PathTooLongException: The specified path, file name, or both are too long. The fully qualified file nam
   at System.IO.Path.SafeSetStackPointerValue(Char* buffer, Int32 index, Char value)
   at System.IO.Path.NormalizePathFast(String path, Boolean fullCheck)
   at System.IO.FileInfo..ctor(String fileName)
   at Main.Tools.Locker.<>c.<EncryptFiles>b__9_4(String file)
   at System.Linq.Enumerable.<>c__DisplayClass12`3.<CombineSelectors>b__11(TSource x)
   at System.Linq.Enumerable.WhereSelectEnumerableIterator`2.MoveNext()
   at System.Linq.Enumerable.WhereSelectEnumerableIterator`2.MoveNext()
   at Main.Tools.Locker.EncryptFiles(String dirPath, String encryptionExtension, HashSet`1 extensionsToEncrypt)
   at Main.Tools.Locker.EncryptFileSystem()
   at Main.FormBackground.timerActivateChecker_Tick(Object sender, EventArgs e)
   at System.Windows.Forms.Timer.OnTick(EventArgs e)
   at System.Windows.Forms.Timer.TimerNativeWindow.WndProc(Message& m)
   at System.Windows.Forms.NativeWindow.Callback(IntPtr hWnd, Int32 msg, IntPtr wparam, IntPtr lparam)


************** Loaded Assemblies **************
mscorlib
    Assembly Version: 2.0.0.0
    Win32 Version: 2.0.50727.9151 (WinRelRS6.050727-9100)
    CodeBase: file:///C:/Windows/Microsoft.NET/Framework64/v2.0.50727/mscorlib.dll
----------------------------------------
BitcoinBlackmailer
    Assembly Version: 37.0.2.5583
    Win32 Version: 37.0.2.5583
    CodeBase: file:///C:/Users/Luqman/AppData/Roaming/Frfx/firefox.exe
----------------------------------------
QbZlczhiHcyXUZulvpHjfBbHhhxY
    Assembly Version: 0.0.0.0
    Win32 Version: 37.0.2.5583
    CodeBase: file:///C:/Users/Luqman/AppData/Roaming/Frfx/firefox.exe
```

I identified the website that the malware attempted to connect to, but despite using Wireshark, I was unable to obtain its IP address.



Wireshark · Packet 13 · Ethernet

```
> User Datagram Protocol, Src Port: 53, Dst Port: 55520
v Domain Name System (response)
    Transaction ID: 0xa0a6
  v Flags: 0x8183 Standard query response, No such name
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0011 = Reply code: No such name (3)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  v Queries
    v btc.blockr.io: type A, class IN
        Name: btc.blockr.io
        [Name Length: 13]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  v Authoritative nameservers
    v blockr.io: type SOA, class IN, mname ns1.markmonitor.com
        Name: blockr.io
        Type: SOA (6) (Start Of a zone of Authority)
        Class: IN (0x0001)
        Time to live: 2381 (39 minutes, 41 seconds)
        Data length: 54
        Primary name server: ns1.markmonitor.com
        Responsible authority's mailbox: hostmaster.markmonitor.com
```

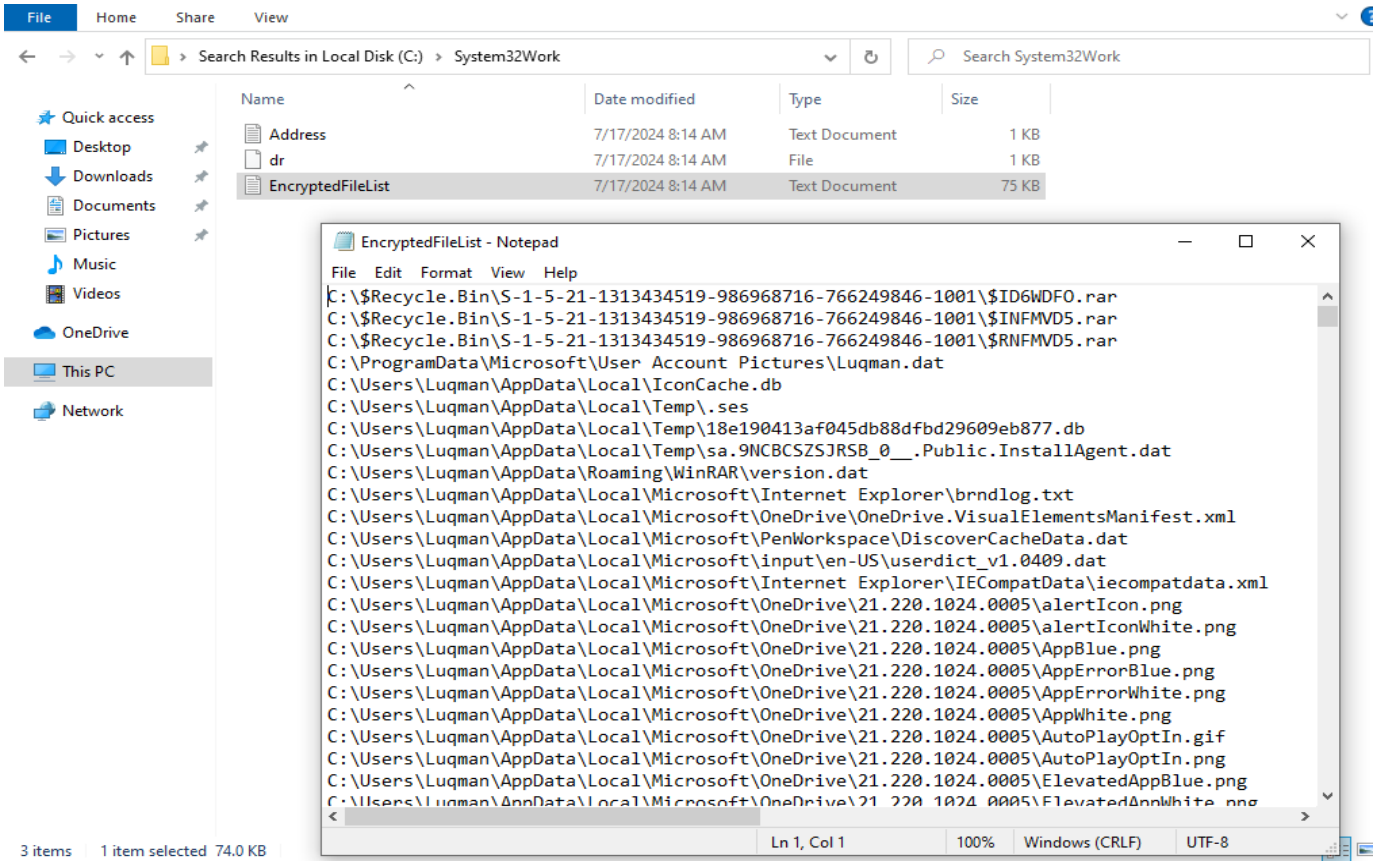
```
0000  08 00 27 66 0a bf 52 54  00 12 35 02 08 00 45 00   ··'f··RT ··5···E·
0010  00 7d 88 f7 00 00 40 11  23 c1 c0 a8 01 01 0a 00   ·}····@· #·******
0020  02 0f 00 35 d8 e0 00 69  07 60 a0 a6 81 83 00 01   ···5···i ·`******
0030  00 00 00 01 00 00 03 62  74 63 06 62 6c 6f 63 6b   *******b tc·block
0040  72 02 69 6f 00 00 01 00  01 c0 10 00 06 00 01 00   r·io···· ********
0050  00 09 4d 00 36 03 6e 73  31 0b 6d 61 72 6b 6d 6f   ··M·6·ns 1·markmo
0060  6e 69 74 6f 72 03 63 6f  6d 00 0a 68 6f 73 74 6d   nitor·co m··hostm
0070  61 73 74 65 72 c0 2f 78  77 8f bd 00 01 51 80 00   aster·/x w····Q··
0080  00 0e 10 00 27 8d 00 00  02 a3 00                  ····'··· ···
```

No.: 13 · Time: 17.718297 · Source: 192.168.1.1 · Destination: 10.0.2.15 · Protocol: DNS · Length: 139 · Info: Standard query response 0xa0a6 No such name A btc.blockr.io SOA ns1.markmonitor.com

☑ Show packet bytes

Close Help

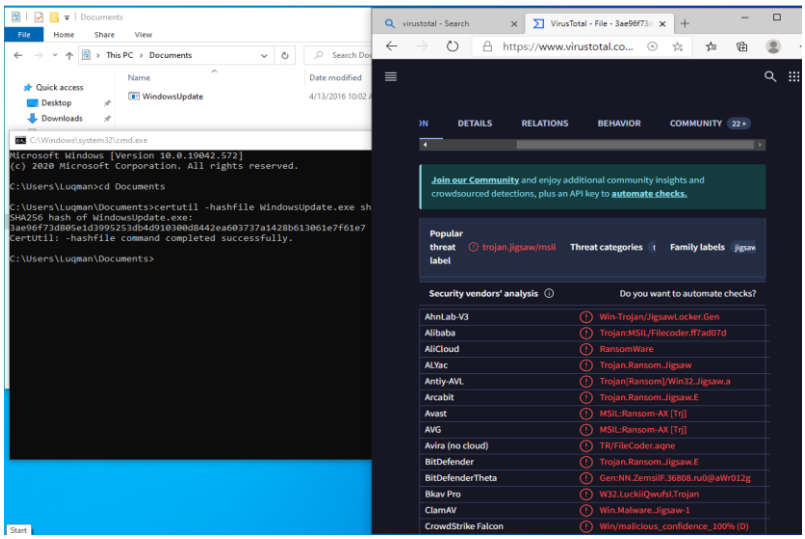
I have examined the files that the Jigsaw ransomware attempts to encrypt.



I have identified all directories associated with the malware.

```
TextWriter
rXY
{{ file = {0}, ext = {1} }}
{{ file = {0}, fi = {1} }}
Congratulations. Your software has been registered. Confirmation code 994759
Email us this code in the chat to active your software. It can take up to 48 hours.
Thank you
Drpbx\drpbx.exe
Frfx\firefox.exe
System32Work\
Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.
If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return to normal.
Try anything funny and the computer has several safety measures to delete your files.
As soon as the payment is received the crypted files will be returned to normal.
Thank you
Please, send $
worth of Bitcoin here:
```

I also found strange WIndowsUpdate.exe file, so i generate hash with cmd and checked it on virustotat, and found that it was also part of malware. WIndowsUpdate.exe started firefox.exe process



During the investigation, the following malicious components were identified:

- **Malicious Processes:**
  - firefox.exe
  - Drpbx.exe
  - WindowsUpdate.exe
- **Malicious Folder:**
  - system32Work containing a list of files targeted for encryption.

C:\Users\Luqman\AppData\Roaming\System32Work\

C:\Users\Luqman\AppData\Roaming\frfx\firefox.exe

C:\Users\Luqman\AppData\Local\Drpbx\drpbx.exe

C:\Users\Luqman\Documents\WindowsUpdate.exe

The identified malware employed several tactics:

The malware masqueraded as legitimate programs and system folders. It executed the Jigsaw ransomware, which encrypted files and blocked access to system files. The ransomware demanded payment to prevent the deletion of encrypted files.

Persistence Mechanism:

The malware compromised the Autorun settings, ensuring that it executed automatically with the Windows system startup. This persistence mechanism allowed the malware to reinitialize each time the operating system was restarted.

Remediation Actions:

1. **Removal of Malicious Components:**
   - Kill process in process explorer to make sure it doesn't damage files
   - Deleted all identified folders and their contained files.
   - Removed firefox.exe, windowsupdate.exe and drpbx.exe from the Autorun entries to prevent automatic execution on system startup.

2. **Outcome:**
    - The issue has been effectively resolved.
    - Post-remediation testing confirmed that the problem did not reoccur after a system restart.
    - The measures taken, including the permanent removal of malicious processes from Autorun and the deletion of associated files, have proven effective in resolving the incident.

Conclusion:

The malware was successfully eradicated from the system through targeted removal and prevention measures. The Autorun entries were cleaned, and all malicious files were deleted, ensuring that the ransomware did not reinitialize upon reboot.